Claims:

1. (Currently Amended) A computer implemented method comprising:

establishing, via the computer, at least one cryptography service parameter threshold comprising a minimum level of security;

establishing, via the computer, at least one maximum cryptography service parameter threshold;

wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes establishing a plurality of correctness categories, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier and said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories consisting of authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms;

selectively detecting, via the computer, a request from an application submitted via an application programming interface to an operating system of the computer, the request comprising a request for at least one cryptography service at the computer; and

selectively performing, via the computer, at least one correctness detection action responsive to detecting the request based on the requested

cryptography service and the at least one cryptography service parameter threshold, wherein[[;]] :

the at least one correctness detection action selectively performed includes suggesting at least one alternative cryptography service;

the at least one alternative cryptography service comprises a cryptography service which meets the minimum level of security; and

the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold, wherein the size of the cryptographic key is identified by bit length.

2. (Currently Amended) The computer implemented method as recited in Claim 1, wherein establishing, via the computer, said at least one

cryptography service parameter threshold includes at least identifying unacceptable cryptography algorithms.

3. (Currently Amended) The computer implemented method as recited in Claim 1, wherein establishing, via the computer, said at least one cryptography service parameter threshold includes at least identifying acceptable cryptography algorithms.

4 - 7. (Canceled)

8. (Currently Amended) The computer implemented method as recited in Claim 1, wherein establishing, via the computer, said at least one cryptography service parameter threshold includes at least identifying at least one acceptable seed size parameter.

9. (Currently Amended) The computer implemented method as recited in Claim 1, wherein establishing, via the computer, said at least one cryptography service parameter threshold includes at least identifying at least one unacceptable seed size parameter.

10. (Currently Amended) The computer implemented method as recited in Claim 1, wherein selectively detecting, via the computer, said request for at least one cryptography service includes monitoring at least one process selected from a group of processes comprising an application, an operating system, a cryptography system service, and another process calling into the cryptography application programming interfaces.

11 - 12. (Canceled)

13. (Currently Amended) The computer implemented method as recited in Claim 1, wherein selectively performing, via the computer, said at least one correctness detection action based on said requested cryptography service and said at least one cryptography service parameter threshold includes determining if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

14. (Currently Amended) The computer implemented method as recited in Claim 13, wherein determining if said cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold further includes

comparing a cryptography algorithm identifier with said at least one cryptography service parameter threshold.

15. (Currently Amended) The computer implemented method as recited in Claim 1, wherein selectively performing, via the computer, said at least one correctness detection action based on said requested cryptography service and said at least one cryptography service parameter threshold includes performing at least one action selected from a group of actions consisting of ~~a plurality of actions, the plurality of actions comprising~~:

interrupting at least one process;

stopping at least one process;

starting at least one process;

displaying alert information;

logging alert information;

suggesting at least one alternative cryptography service;

outputting alert messages;

causing alteration of a graphical user interface; and

forcing use of at least one other cryptography service.

16. (Currently Amended) A computer readable medium having computer-implementable instructions embodied thereon, which when executed cause one or more processing units to perform acts comprising:

establishing at least one cryptography service parameter threshold comprising a minimum cryptography service parameter threshold;

establishing at least one maximum cryptography service parameter threshold;

wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes establishing a plurality of correctness categories, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier and said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories consisting of authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms;

selectively detecting a request from an application submitted via an application programming interface to an operating system, the request comprising a request for at least one cryptography service; and

selectively performing at least one correctness detection action responsive to detecting the request based on said requested cryptography service and said at least one minimum cryptography service parameter threshold and said at least one maximum cryptography service parameter threshold, wherein:

the at least one correctness detection action selectively performed includes forcing use of at least one alternative cryptography service;

the at least one alternative cryptography service comprises a cryptography service which meets the minimum level of security; and

the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold, wherein the size of the cryptographic key is identified by bit length.

17. (Canceled)

18. (Previously Presented) The computer readable medium as recited in Claim 17, wherein establishing said at least one of either said minimum

or maximum cryptography service parameter threshold includes at least one of the following acts:

identifying unacceptable cryptography algorithms; and

identifying acceptable cryptography algorithms.

19. (Previously Presented) The computer readable medium as recited in Claim 17, wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes at least one of the following acts:

identifying at least one unacceptable cryptography key size parameter; and

identifying at least one acceptable cryptography key size parameter.

20 - 21. (Canceled)

22. (Previously Presented) The computer readable medium as recited in Claim 17, wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes at least one of the following acts:

identifying at least one acceptable seed size parameter; and

identifying at least one unacceptable seed size parameter.

23. (Original) The computer readable medium as recited in Claim 16, wherein selectively detecting said request for at least one cryptography service includes monitoring at least one process selected from a group of processes comprising an application, an operating system, a cryptography algorithm, and a cryptography application programming interface.

24. (Original) The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes determining if a cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

25. (Original) The computer readable medium as recited in Claim 24, wherein determining if said cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold includes comparing a size of said cryptographic key with said at least one cryptography service parameter threshold.

26. (Original) The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes determining if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

27. (Original) The computer readable medium as recited in Claim 26, wherein determining if said cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold further includes comparing a cryptography algorithm identifier with said at least one cryptography service parameter threshold.

28. (Currently Amended) The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes performing at least one action selected from a group of actions ~~comprising~~ consisting of: interrupting at least one process,

stopping at least one process, starting at least one process, displaying alert information, logging alert information, suggesting at least one alternative cryptography service, outputting alert messages, and causing alteration of a graphical user interface.

29. (Currently Amended) An apparatus comprising:

a system memory;

a processing unit; and

cryptography correctness detection logic configured to:

establish at least one cryptography service parameter threshold, wherein the at least one cryptography service parameter threshold comprises a threshold setting a minimum level of security;

establish at least one maximum cryptography service parameter threshold;

maintain said at least of said minimum and maximum one cryptography service parameter thresholds in said memory; and

establish a plurality of correctness categories in said memory, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier wherein said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories consisting of

authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms;

selectively detect a request for at least one cryptography service; and

selectively perform at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy the at least one cryptography service parameter threshold, wherein the at least one correctness detection action selectively performed includes forcing use of at least one other cryptography service, wherein the at least one other cryptography service comprises a cryptography service having a higher level of security than represented by the cryptography service parameter threshold.

30. (Canceled)

31. (Original) The apparatus as recited in Claim 30, wherein said cryptography correctness detection logic is further configured to identify at least one of the following: at least one unacceptable cryptography algorithm, and at least one acceptable cryptography algorithm.

32. (Original) The apparatus as recited in Claim 30, wherein said cryptography correctness detection logic is further configured to identify at least

one of the following: at least one unacceptable cryptography key size parameter; and at least one acceptable cryptography key size parameter.

33. (Canceled)

34. (Original) The apparatus as recited in Claim 30, wherein said cryptography correctness detection logic is further configured to identify at least one of the following:

at least one acceptable seed size parameter; and

at least one unacceptable seed size parameter.

35. (Original) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to monitor at least one process selected from a group of processes comprising an application, an operating system, a cryptography algorithm, and a cryptography application programming interface.

36. (Original) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to determine if a cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

37. (Original) The apparatus as recited in Claim 36, wherein said cryptography correctness detection logic is further configured to compare a size of said cryptographic key with said at least one cryptography service parameter threshold.

38. (Original) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to determine if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

39. (Original) The apparatus as recited in Claim 38, wherein said cryptography correctness detection logic is further configured to compare a cryptography algorithm identifier with said at least one cryptography service parameter threshold.

40. (Currently Amended) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to use at least one action selected from a group of actions ~~comprising~~ consisting of:

interrupting at least one process,

stopping at least one process,

starting at least one process,

displaying alert information,

logging alert information,

suggesting at least one alternative cryptography service,

outputting alert messages, and

causing alteration of a graphical user interface, to be performed.

41. (Previously Presented) The method as recited in Claim 1, wherein:

in an event that the cryptography service is an asymmetric cryptography service, the minimum level of security comprises a minimum acceptable public key size of at least 1024 bits; and

in an event that the cryptography service is a symmetric cryptography service, the minimum level of security comprises a minimum acceptable symmetric key size of at least 128 bits.

42. (Previously Presented) The computer readable medium as recited in Claim 16, wherein:

the at least one alternative cryptography service comprises a cryptography service which meets the minimum level of security; and

the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold, wherein the size of the cryptographic key is identified by bit length.

43. (Previously Presented) The apparatus of claim 29 wherein the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold

includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold, wherein the size of the cryptographic key is identified by bit length.) The method as recited in Claim 1, wherein:

in an event that the cryptography service is an asymmetric cryptography service, the minimum level of security comprises a minimum acceptable public key size of at least 1024 bits; and

in an event that the cryptography service is a symmetric cryptography service, the minimum level of security comprises a minimum acceptable symmetric key size of at least 128 bits.